ISAC CYTOMETRY Journal of Quantitative Cell Science PART A

Critical Steps in Data Management During a Crisis

Michele Black,[1*] Karla Moncada,[2] Kyle Herstad[1]

FLOW cytometry SRLs are tasked with a wide array of responsibilities and providing technical knowledge to users to ensure high-quality data is an essential function. It is critical to have standard operating procedures (SOP's) to protect the workstations generating the data and a formal system to manage and back up the data. When writing and implementing SOP's, there are multiple considerations to take into account. The possibility of data corruption and accidental deletion of data is at the core of the concerns and usually serves as a starting point of the thought process for making these preparations. However, there are other circumstances to consider in data management. Natural disasters and unforeseen conditions that arise, such as the current pandemic, pose a threat to data management, and considerations for these events is crucial when making a data management plan. There are four interconnected stages to managing an emergency: mitigation, preparedness, response, and recovery; lessons learned through one emergency may help plan and respond in the future (1). Emergency planning is essential to meet the challenges introduced by disaster situations, which can physically destroy data. Evaluating what situations could impact data integrity and implementing practices to mitigate them will ensure that the SRL is prepared and can respond in an emergency or, better yet, eliminate a potential disaster from happening. Mitigation efforts aim to limit an emergency's effect while the response and recovery aid in restoring what was affected or lost and provide an opportunity for improvement. The loss due to floods, fire, or other natural disasters, requires a system that keeps data backed up off-site. SRLs in regions prone to natural disasters have already experienced these challenges; Tulane university faced the difficult reality of the need to backup essential data off-site in the wake of Hurricane Katrina (2). Lessons learned from having locally stored data lost due to widespread damage to buildings have led to implementing systems for keeping data off-site out of the same geographical area to withstand a large-scale disaster. A comprehensive data management plan (Table 1) will prepare for potential threats to the hardware systems where data are collected and stored and respond by implementing practices that safeguard instrument workstations from data loss or corruption, including antiviral and malware software, restricting access to the Internet, and limiting external device connections. Other important considerations revolve around managing information related to raw data files that give data relevance and context, which we will discuss later.

Research laboratories across the globe experienced the pandemic's impact. Information obtained through the ISAC SRL COVID-19 survey shows that many institutions began operating with new social distancing rules that included limited contact with others, staggered nonoverlapping work schedules, and working from home when possible (3). SRLs that were shutdown or had limited onsite personnel faced the obstacle of accessing data and managing instrument workstations while working from home. Even as some SRLs were deemed essential to the current crisis and continued working onsite, prolonged staffing limitations resulted in some data management challenges. Most SRL's experienced an expanded need for remote access to copy or analyze data and perform routine maintenance of instrument workstations. Additional challenges revolved around the reliable automated storage of data. SRLs with robust data management systems in place before the pandemic experienced fewer barriers to uninterrupted data

[1]Department of Immunology, University of Washington, Seattle, Washington

[2]UT Health San Antonio, Texas

Received 21 August 2020; Revised 31 October 2020; Accepted 11 November 2020

Additional Supporting Information may be found in the online version of this article.

*Correspondence to: Michele Black, Department of Immunology, University of Washington, 750 Republican St. Seattle, WA 98109, USA
Email: mblack2@uw.edu

Published online in Wiley Online Library (wileyonlinelibrary.com)

DOI: 10.1002/cyto.a.24265

Table 1. Data management plan

PROBLEM	SOLUTION
Loss of data	• Automate data copy/transfer to a secure location • Storage in the cloud or off-site • Data redundancy: copy in two locations • Protect against accidental deletion: read/write permissions
Access to data	• Remote access: cloud storage, secure server, or VPN
Difficulties with sharing data	• Data organization (user or laboratory-based folders) • Data access permission: Ability to invite users, PI's, or collaborators to a specific folder or file
Data accumulation and machine maintenance	• Scheduled routine data cleanup: Disk cleanup and Defrag • Backup databases and remove old experiments • Up-to-date Antivirus/ malware • Limit USB/external HD and Internet access
Data removal	• Verification data are saved in long-term storage • Automate data deletion • Remote access to verify and to delete data
Lack of annotation/ metadata	• SRL training and education program

Developing a SRL data management plan that addresses the problems related to protecting data integrity and the machines used to collect it is essential. The solutions presented can help meet best practices while also creating a plan for emergencies and mitigating disruptions to the data collection, analysis, and preservation when normal operations are not possible.

management. However, the pandemic exposed weaknesses in SRLs who had not incorporated an emergency preparedness plan into their operations. For SRLs without a comprehensive data management system, implementing a strategy that takes advantage of remote instrument access, automated data transfer, and cloud-based storage could help alleviate future issues.

Developing a universal standardized data management system is not entirely possible since data management policies vary among SRLs. Depending on the setting, that is, Pharma or clinical laboratories, the regulatory requirements can restrict how data are shared or stored. SRLs with limited funds and resources may have to limit the scope of what is possible when establishing a data management system. A simple approach in some SRLs requires the user to self-manage their collected data. By placing the responsibility of data management on the user, it decreases the burden on the SRL. However, this approach comes with risks. Users that do not have a good backup strategy could lose data that would not be recoverable. Additionally, allowing users to copy data from instrument workstations directly to thumb drives or external hard drives could lead to malware and viruses. In the best interest of the SRL, policies that protect instrument workstations and provide measures to maintain workstation health should be in place. Instrument workstations are expensive and essential to the functionality of the cytometer. These workstations should collect data exclusively and not be used for storage because there is a risk of corrupting data files or instrument software. Allowing users to connect to a remote server or cloud storage is a safer alternative. Many SRLs are required to maintain a backup of raw data because it is considered the institutions' intellectual property and falls in line with best practices to support investigators. There are different approaches to safeguarding data that depend on institutional policies and resources. The goal is to ensure its integrity and accessibility. Implementing processes that mitigate the impact of situations outside of the SRL's control help protect data.

As technology advances, data management methods should evolve, with SRLs continuing to refine data management and backup protocols. Some SRLs have formed collaborations with local IT and bioinformatics resources to support data management and backup. Others have purchased third party data management solutions that come as a package to preserve and distribute data. The post-COVID-19 data management survey (Fig. 1) revealed most SRLs that responded have an in-house solution for data management. Of those surveyed, only three SRLs used a commercial data management product. Half of the respondents indicated that the long-term data storage was the responsibility of the SRL, even if users were also required to handle exporting and copying data to their own storage device. Over half indicated that data are manually copied or moved from the instrument workstations to a network location, physical media like USB, CD, or external hard drive. Challenges reported relating to the pandemic were all attributed to slow VPN connections and no remote access, with only two laboratories indicating a need to change standard data management practices in response to the pandemic. SRLs with automated systems or reliable remote access to their instrument workstations reported that they were not affected adversely with shutdowns due to COVID-19. The overall takeaway from the survey is that having a system that allows for remote access to instrument workstation, automated data backup and remote access to collected data for the users enhances the ability to support a functional SRL, even when there is a significant interruption in normal operations. Here, we highlight two such solutions for data management that worked successfully during the pandemic. One solution was developed internally by the SRL and takes advantage of institutional unlimited data storage. The second is an institutional IT system that the SRL leveraged to aid in data backup and storage.

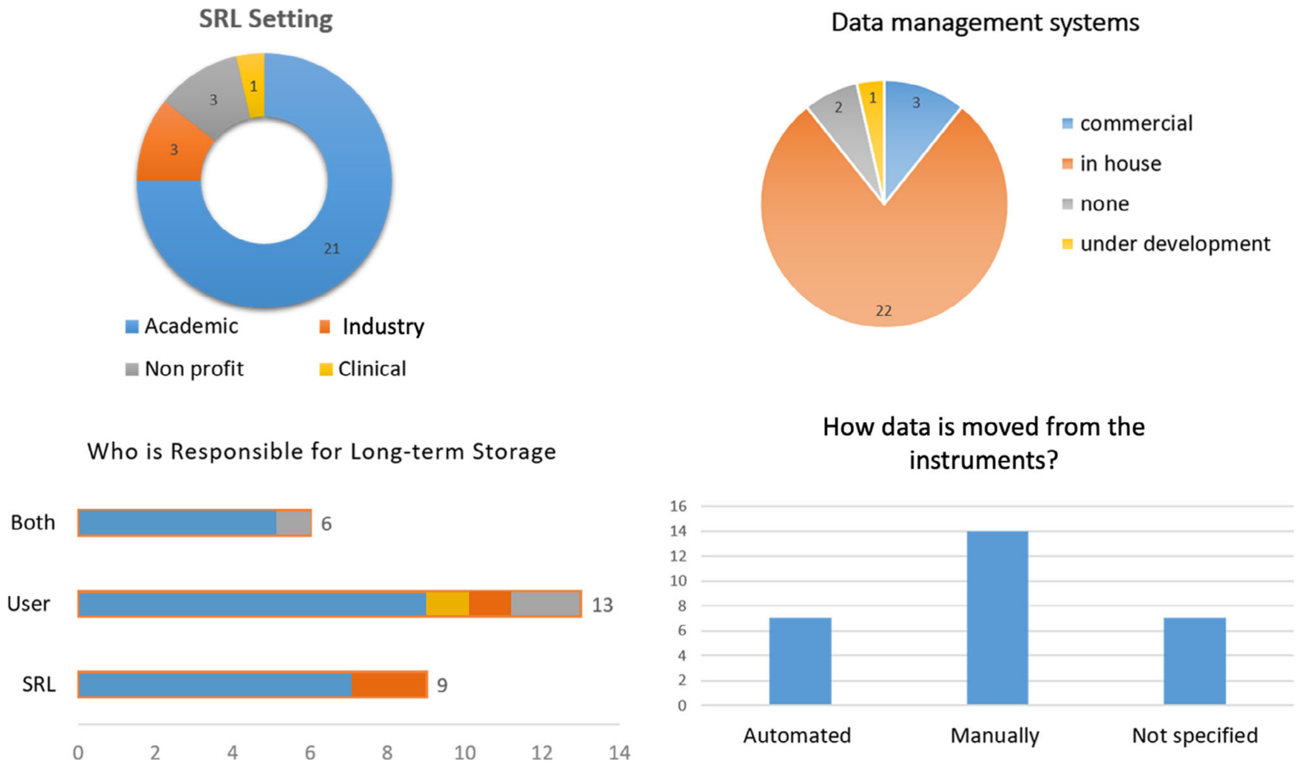

Figure 1. Results from the COVID-19 data management survey with 28 respondents. Twenty-one of the 28 respondents are in academic settings. The majority of all respondents have in-house solutions for data management. The SRL is responsible for long-term storage in over half of the labs that responded, with users being solely responsible in 13 of the 28 laboratories. Automated data transfer was reported in only 25% (7 out of the 28) of SRLs surveyed. Only two of the 28 respondents indicated that the pandemic impacted their standard method for data management.

Two Data Management Stories

The Cell Analysis Facility (CAF) Shared Resource Lab at the University of Washington Seattle uses automated script-based processes in the SRL, including data transfer systems. These processes alleviate repetitive tasks and increase consistency for data management. Automated processes aid staff and users by providing an efficient method to manage data even when staff is not available. As technology has evolved and complex multiparameter assays have become standard, the amounts of cytometry data stored and managed by the SRL have increased. Advancements in data storage technology have also improved speed and accessibility while becoming cheaper to store. The most recent update to the data management system in the CAF SRL occurred at the beginning of 2020 and coincided with the COVID-19 related shutdowns. The CAF was retiring an obsolete and expensive server hosted that cost $10,000 to purchase and set up with a maintenance cost of $500/month. While adequate for backing up and safeguarding data, the server was not ideal with a complicated process to access data. The Cell Analysis Facility began looking at data storage alternatives that would be more cost-effective and user-friendly for both the end-user to access data and the staff to administer. The solution chosen was a cloud-based data repository that allows users of the facility to access their data remotely from any computer with an Internet connection and easily share data with their collaborators.

The University of Washington hosts an implementation of Google G Suite for Education (Mountain View, CA) as part of its mission to provide a quick, easy, and user-centered collaborative environment. The university funds this through the Technology Recharge. The SRL pays a nominal fee of $115/month as part of operational overhead. Google Drive (GD) provides free unlimited storage to all students, staff, and faculty. The SRL took advantage of this feature to store data generated in its facility. One approach to utilizing GD to store cytometry data could require all users to log in to their own G Suite account and manually copy their data into their GD. However, that approach ignores the potential issues with data preservation and retrieval; for example, if a user separates from the institution or inadvertently deletes data, recovery could be difficult or impossible. To adhere to the best practices for data management, a system that centrally stores data and is accessible even if an investigator separates from the institution is preferred. The following solution leveraged the data storage and Application Programming Interface (API) in the UW G Suite account to host the facility's data.

The CAF has created a system that ties each user to an ID for data management and tracking. The system utilizes the University Network ID (UWNetID) to link each user account to the SRL with their UW email address. The account takes advantage of authentication to secure access to the scheduling calendar and the users' data. It is also used as their account login ID to the acquisition software on the instrument workstations, becomes the folder name for their collected data, and is used to track billing. Having a user ID that ties to all these components together aids in instrument data management and all other data associated with each user from communication to compliance of documenting training. Setting up a new user involves a series of forms and scripts that establish an account with automated email communication (Fig. 2). With their account, they can access the scheduling calendar and reserve time to use the facility's services. During facility orientation and training, the staff creates a login account based on the UWNetID for the instrument acquisition software and sets up a folder to automatically export and save the .fcs files while collecting data. The data then automatically upload to the GD data repository by the upload script scheduled to run at regular intervals. The CAF instructs users to organize the data they collect in a logical way that best meets their downstream analysis needs and advises them to adhere to a naming structure that will make the data folders and files easily identifiable in the future. The GD data repository is managed by a "Python (PY) data upload script" that checks for new files within specified directories on the instrument workstations and uploads any new files it detects to the CAF's GD (see supplemental data S1 and S2). The file structure that each user sets up on the cytometer computers is recreated on GD and organized by folders with the user login ID. The PY script loops at 2-min intervals and runs through the network locations specified in the config file for each loop, checking every folder and file in the directory against a tree data structure that tracks all file uploads and file structure. If the script comes across a folder or file that is not present in the tree, it is created or uploaded to GD and added to the tree. When a new user folder uploads to the GD, the script then shares the new user folder with the associated UWNetID email address sending them an email with a link to access (Fig. 3). The "PY data upload script" manages all data recorded on the instrument workstations while a "config file" specifies the network locations that the script checks for data generated on the cytometers. The SRL has the flexibility to add access permissions of other people, such as the PI or collaborators, to any user folder or subfolder by request. The SRL can assist users with data analysis and share results by uploading them to the user's GD folder. The user permission for the raw .fcs files is set to read-only to protect the data from accidental deletion. For external users, their data are exported and stored in the SRL UWNetID "flowlab" organized in subfolders by institution then user. SRL staff can grant permission to users outside the UWNetID system to securely access subfolders containing collected data. The CAF system does not integrate with data collected at other UW SRLs. There is no University-wide system to coordinate

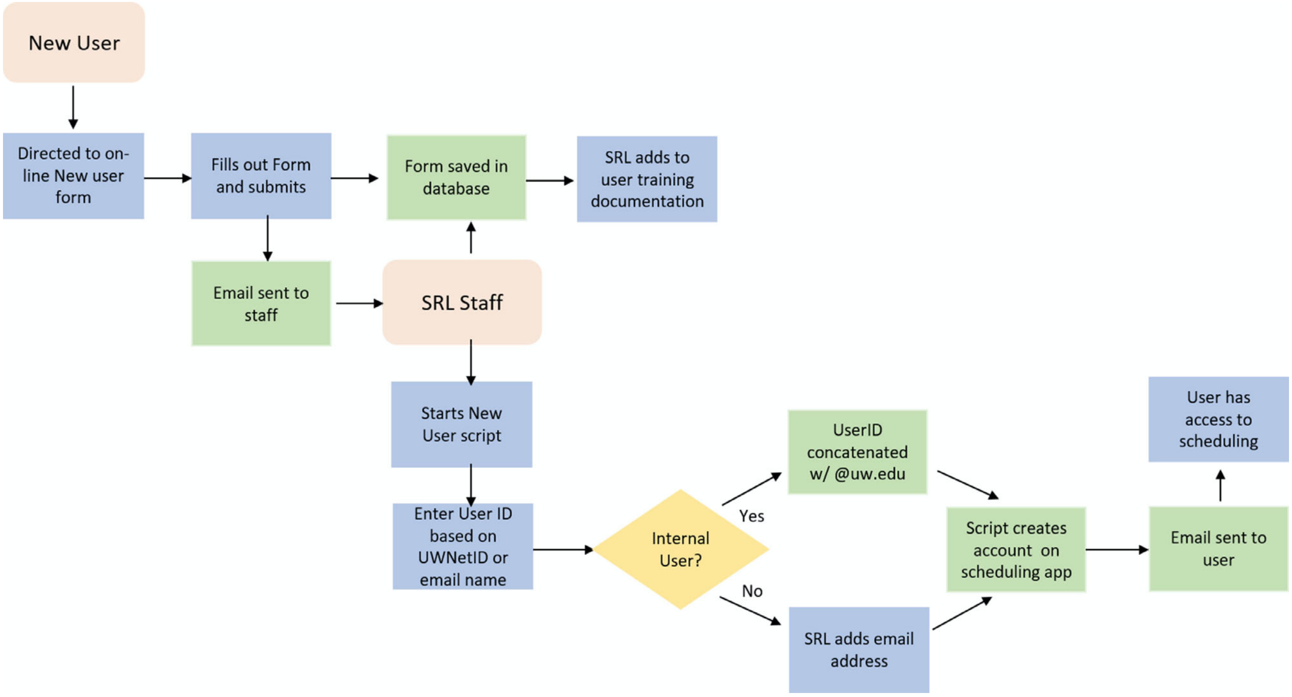
New User
Directed to on-line New user form
Fills out Form and submits
Form saved in database
SRL adds to user training documentation
Email sent to staff
SRL Staff
Starts New User script
Enter User ID based on UWNetID or email name
Internal User?
Yes
No
UserID concatenated w/ @uw.edu
SRL adds email address
Script creates account on scheduling app
Email sent to user
User has access to scheduling

Figure 2. Workflow for adding new users: SRL staff initiate an automated script when a user fills out the request form to establish an account. When the script runs, it creates an account to grant permission to the scheduling program and send an email to the user with directions on how to use the scheduling calendar to book instrument time and training. The account established with the user's UWNetID is used to track all user processes, including managing user data, granting permission and access to software, and administrative functions like tracking training and billing.

between the multiple Schools, Departments, and SRLs. Users can download and manage data on their own storage devices that integrate into their Laboratory's research program.

The CAF complies with disaster preparedness plans by having a secondary data backup in the unlikely situation of a catastrophic event on the GD repository. A robocopy script runs daily to create a secondary copy of the stored data on three-10 Tb storage drives in master folders organized by user UWNetID. The CAF data retention policy on the local secondary archive is for no less than 7 years.

Remote access by CAF staff to a central workstation allowed monitoring the automation scripts and provided secure access to each instrument workstation to ensure that data transfer was successful. Researchers reported ease of access to data that helped them perform data analysis from home. Most researchers use the FCM software FlowJo™ (Ashland, OR) at the UW, typically located on a laboratory workstation. For those working from home, they were able to download a 30-day free trial of FlowJo or request their UW site license to be moved to FlowJo Portal to give them more flexibility for where they could analyze data. The GD system has proven reliable while keeping the facility running smoothly when SRL staff is limited or not onsite. Overall, SRL has benefited from more automation and better remote access.

One challenge presented during the pandemic involved deleting older data from instruments. The SRL staff work nonoverlapping schedules, and the time-intensive task of deleting data became difficult with the limited staff presence. Implementing a "data deletion script" to automatically remove data older than 60 days alleviated this issue (see supplemental data S1 and S2). With eight cytometers, having this process automated relieved a time-intensive task, enabling staff to perform other duties. Our only data management processes that are not automated include backing up the database and removing old experiments from the cytometer software. We have yet to find a way to automated this and must still manually perform these functions.

The Flow Cytometry Core Facility (FCCF) at UT Health San Antonio implemented a data backup and management protocol established mainly in collaboration with the systems integration department at UT Health and support from the Vice President for Research (VPR). In 2017, a review of the data management SOP exposed the need for the FCCF to modernize their protocol due to the steady increase in userbase and larger data sets with higher dimensionality being produced, taking advantage of the new technological advancements in data backup and storage. The team assigned to work with the FCCF implemented an in-house managed system to

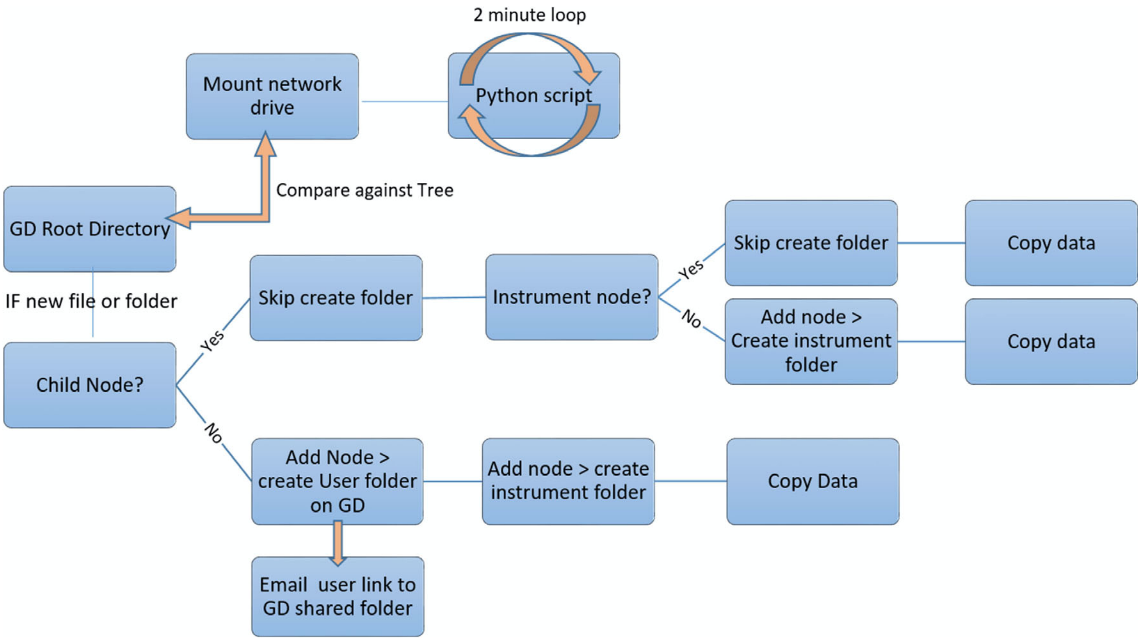

Figure 3. Each workstation exports collected data to a folder path labeled with the user's login ID. The data collected on any of the acquisition software platforms; Becton Dickinson FACSDiva™ software (San Jose, CA), Cytek Spectroflow® (Fremont, CA), and Amnis IDEAS (Seattle, WA) are all set up to follow a similar network path for accessing the data folders. A tree data structure is used to keep track of which files have already been uploaded to Google Drive. Whenever the script finds a new user folder, a child node of the root node is added and has its value set to the name of the folder, which in this case, is the user's UWNetID. A second child node is added under the "user node" and has its value set to the name of the instrument the first-time user was using. Any other instruments used by that individual in the future will be added as child nodes of the "user node." The file structure that the user creates within their folder on the instrument workstations is recreated under the corresponding "instrument node," with nodes created for each folder and file, the file nodes being leaf nodes. Before a folder or file is added to the tree, a request is sent to GD via the GD API to create that folder or upload that file to GD. If the request is successful, the folder or file is added to the tree, so the script knows not to create/upload it again. The ID that GD assigns to the new folder/file is stored in the corresponding node and is used to tell GD where to place child folders/files in the future.

provide the SRL with data backup and storage solutions and a service component that supplies administrative and technical support. The COVID-19 pandemic was the first disaster the FCCF encountered, and the data backup and management protocol have provided users and staff a reliable and efficient way to access their data remotely.

Leased mass storage (LMS) was used to set up a server that users can access with VPN permission. This allows FCCF instrument workstations to connect directly to the server to export data after each experiment. Staff and users can also login to the server and access data remotely for analysis on designated analysis workstations or private computers. The FCCF supports cloud licenses for analysis software available for individual user subscriptions. This allows users to install analysis software on off-site computers to analyze data while working remotely.

While the LMS covers essential file services, the systems integration department also ensures daily storage backups and supplies troubleshooting support. Backups are kept off-site on a Dell Isilon storage cluster called the Advanced Data Center (ADC) in Round Rock, TX (*Fig*. 4). It has built-in redundancy to keep data protected and takes daily snapshots at 11 p.m. that are stored for 2 weeks and a weekly off-site replication stored for 4 weeks. The storage location is at the University Data Center (UDC) located at UT Austin, where new FCCF data are being consolidated with the previous backup and stored indefinitely. This SOP provides a higher level of reliability than the FCCF had ever had before. Data stored off-site and duplicated ensures it is recoverable in case of corruption and any unexpected disasters that can pose a threat to local clusters.

The FCCF is currently storing about 5 TB of data and produces an average of 0.5–0.8 TB of data per year and is paying $1,680/year for backup and storage of 5 TB of data ($336/TB). The SRLs at UT Health San Antonio are under the direction of the office of the Vice President of Research. The VPR supplies the local storage space and will allocate extra space as capacity is approached. Many of the other SRLs at UT Health San Antonio are looking into options available as their data backup and storage needs grow. The SOP developed by the FCCF serves as a model approach for other SRLs at the institution. Keeping abreast of novel technology will keep the data management and backup SOP as efficient as possible while mitigating costs that will end up being carried by facility users through chargeback fees.

Data management, on the other hand, is currently implemented manually by the SRL staff. As files are created or upon completion of the experiment, users must export their data to the ADC for backup outside of the acquisition software in which they are created. The duplication of data on the instrument workstation's local drive helps mitigate data loss by accidentally deleting data before exporting, software crashing, or file corruption. Once data have been exported and confirmed to have maintained integrity, the staff is safe to delete data from the instrument workstation.

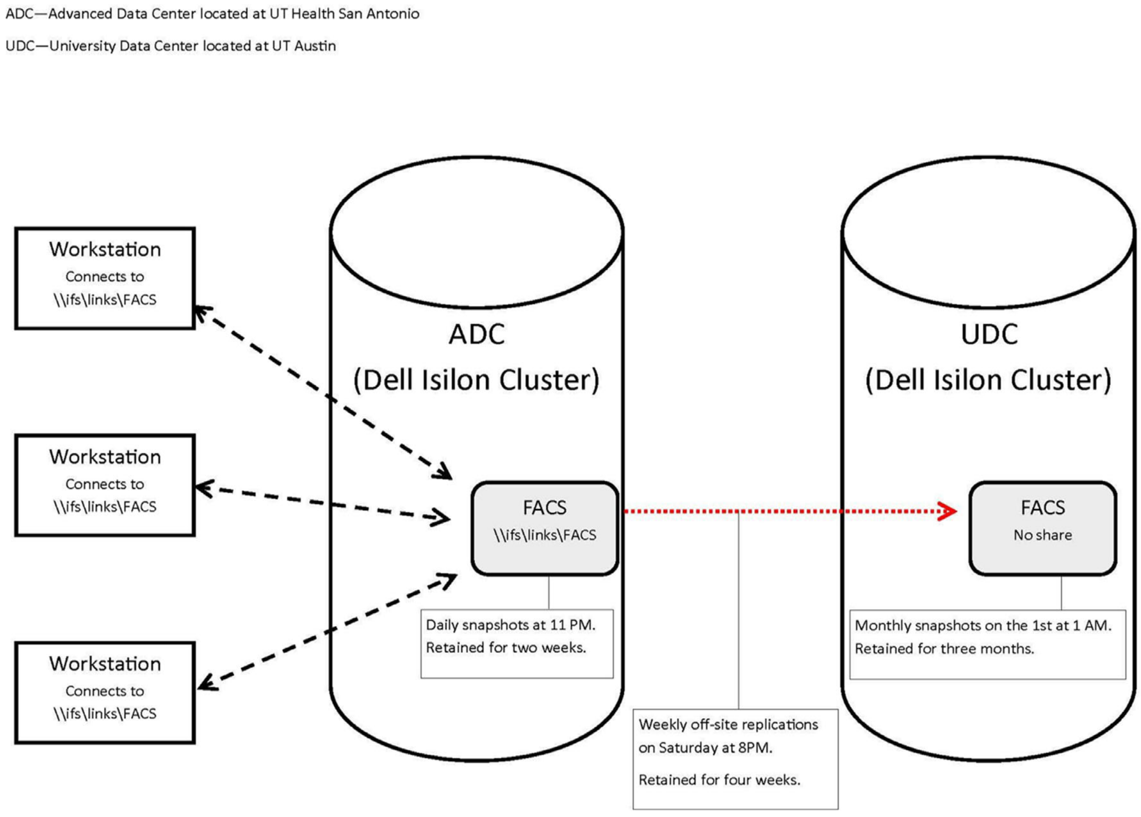

Figure 4. Data backup and storage pathway at UT Health San Antonio.

Although this does create a temporary duplication of data on the instrument workstation, the protocol details the following timeline to manage the data. Once a week, staff will confirm that the data have been exported for backup to the Dell Isilon cluster. Once data backup is confirmed, the staff deletes the user data from the workstation hard drive and acquisition software. This is necessary to maintain hardware and software integrity, data security, and prevent data loss. With staff availability limited onsite to mitigate potential exposure to and from the users during the pandemic, it is important to implement strategies that reduce the chances of falling behind in data management that would result in too much data on the instrument workstation and acquisition software. Software freezing or crashing may require reinstallation of software to restore functionality. Other issues such as corruption of data files, corruption of experiment templates, and software lagging in response time while recording data are also common when too much data accumulate in some acquisition software databases. To alleviate these issues, remote access to instrument workstations is key to allow staff to work on data management while a user concurrently runs the instrument and acquires data.

Whereas the current data backup SOP at the UT Health FCCF has been instrumental for the efficient storage and retrieval of data, especially during the pandemic, the current bottleneck is the data management SOP that requires remote access capabilities to the workstations to delete data from the acquisition software efficiently. This is currently being addressed, where staff will be able to log in remotely and manage data by manually confirming the data backup and deleting data from instrument workstations. However, manually managing data, whether remotely or locally, still requires blocking instrument time to allow staff to carry out this SOP. At UT Health FCCF, instruments are utilized at a minimum of 70% capacity in the FCCF, and data can often remain on workstations beyond the recommended time. Therefore, an automated script to delete data from some acquisition software would be preferable.

Summary

In the wake of the COVID-19 pandemic, SRLs are reevaluating strategies for managing their operations at every level. For data management, the immediate concerns revolve around planning and mitigating potential data loss. The SRL settings, policies, regulations, and certifications will dictate what information must accompany the FCM data files. Record keeping data, including quality assurance, instrument maintenance, and SOP's, are part of the data management assessment. Clinical laboratories and laboratories involved in multicenter studies have the added element of coordinating data management across different laboratories, regions, or countries. It is important to note that the two solutions described above are not HIPAA compliant for the security of Protected Health Information (PHI). The cytometry data collected in these SRLs are primarily basic science research; research utilizing clinical samples cannot identify any personal information. Data generated in conjunction with studies involving human subjects must be protected following HIPAA guidelines and stored in a manner that PHI is not compromised (4). Any FCM data made publicly available must have all PHI removed before uploaded for publication or to a data repository (5).

Data backup and management SOPs will vary across SRLs, but the challenges faced will be universal. Just as natural disasters have exposed weaknesses in our past practices, the COVID-19 pandemic is no different. The COVID-19 pandemic has simultaneously impacted SRLs globally, and the nature of this emergency fundamentally changed the way people work and interact. In this crisis, the key issues revolve around the interrupted physical access to the data when it comes to data management. The above examples highlight how having remote storage and automation eliminated interruption in the data management pipeline at these institutions. We recognize that not all SRLs will have access to cloud storage systems for security or other reasons, but some form of off-site storage is essential. We have learned from the COVID-19 pandemic when addressing data management, the importance of forethought on what types of scenarios could lead to data loss and applying the practices to mitigate and prepare for the new challenges it presented.

Natural disasters and hardware failures can result in the loss of physical data. From a data management perspective, the COVID-19 pandemic had a minimal catastrophic impact on data integrity and can serve as a wake-up call that comprehensive emergency preparedness plans should be developed for any scenario. With that in mind, other types of data loss include poorly annotated data that loses context when not accompanied by relevant supporting information. When information related to a dataset required to analyze and interpret data correctly is missing, that data are potentially useless. Data files that lack identifying metadata like antibody labels, informative sample names, including variables such as species, treatment, or cell type, are potentially worthless if the experimental context is lost. In a scenario wherein the researcher who conducted experiments cannot provide the accompanying relevant information, the data and related body of research may be compromised or lost. Part of an SRL data management plan should include providing guidance to researchers on proper data annotations such as MIFlowCyt standards and how to safeguard their data, including sudden departures of personnel or their inability to provide relevant information about FCM data (6).

Ownership of data can involve multiple entities depending on the setting and funding: the sponsoring institution, the funding source, and the PI (7). While the PI may have custody of the data and be responsible for overseeing its management, SRLs have a role in protecting the integrity of the data produced as part of a service paid for by funding. The SRL is one component of the data management puzzle. The broader setting at the institutional level is a crucial resource and partner in integrating with the other data pipelines. Researchers must understand the basic concepts for managing their entire data portfolio. In the SRL, training is a critical step for onboarding staff and users and should include data management as an integral part of the process. SRLs can provide information to educate users about safeguarding data from being separated from other portions of a research project and the importance of data organization and data backup.

Key components of a good data management program include: developing a system that stores data in a minimum of two locations, protecting against loss of relevant supporting information, and security protocols to protect from malicious acts or theft. As discussed above in the two SRL stories, enabling remote logins allows access directly to workstations and is a useful tool to keep SRLs up and running even when staff cannot physically be onsite. Remote access comes with risks, and careful attention to security is needed to assess what security vulnerability could result. Nevertheless, the benefit of remote access to the users and staff will continue beyond the pandemic and is an opportunity to improve the efficiency of research. While other data management approaches may also be successful, our aim here is to provide suggestions and introduce fundamental concepts on data management to SRLs that need to adopt better practices. An SRL's mission is to provide highly technical services in a knowledgeable, timely manner at a reasonable cost, and an essential part of this mission is to stay up-to-date with issues that can affect the SRL. By incorporating SOPs that adapt to the needs of the users, the changing research environment, and new technologies, SRLs will be able to meet any new challenge.

Acknowledgments

The authors would like to thank those that contributed to the technical processes of this manuscript. Robert Simek and Becki Gerwitz, Systems Integration department at UT Health San Antonio, for designing and implementing data backup and storage using the onsite and off-site data clusters. The authors would also like to thank Rui Gardner for his thoughtful suggestions and help to proofread and edit this manuscript.

Author Contributions

Michele Black: Writing-original draft; writing-review and editing. **Karla Moncada:** Writing-original draft; writing-review and editing. **Kyle Herstad:** Software.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Literature Cited

1. National Research Council (US) Committee on Prudent Practices in the Laboratory. Prudent Practices in the Laboratory: Handling and Management of Chemical Hazards: Updated Version. Washington (DC): National Academies Press (US), 2011 Available at: https://www.ncbi.nlm.nih.gov/books/NBK55874/.
2. Krane N, Kevin MD, Kahn MJ, Markert RJ, Whelton PK, Traber PG, Taylor IL. Surviving Hurricane Katrina: Reconstructing the Educational Enterprise of Tulane University School of Medicine. Acad Med 2007;82(8):757–762.
3. ISAC Shared Resource Lab Services Committee. SRL COVID-19 survey results https://cdn.ymaws.com/isac-net.org/resource/resmgr/docs/srl_newsletter/srl_covid-19_survey_results.pdf
4. United States Department of Health & Human Services. Office for Civil Rights Privacy Brief: Summary of the HIPAA Privacy Rule, HIPAA Compliance Assistance. Available at: http://www.hhs.gov/sites/default/files/privacysummary.pdf
5. Spidlen J, Brinkman RR. Use flow repository to share your clinical data upon study publication. Cytom Part B 2018;94B:196–198.
6. Lee JA, Spidlen J, Boyce K, Cai J, Crosbie N, Dalphin M, Furlong J, Gasparetto M, Goldberg M, Goralczyk EM, et al. MIFlowCyt: The minimum information about a flow cytometry experiment. Cytom Part A 2008;73A:926–930. https://doi.org/10.1002/cyto.a.20623.
7. Office of Research Integrity. US Department of Health and Human Services Guidelines for Responsible Data Management in Scientific Research Available at: https://ori.hhs.gov/images/ddblock/data.pdf